Criado por:	Assunto	Versão	Data	Cod
Bruno Ricardo Pin	Política de Senha	1	10/01/2024	MI121

1. Objetivo e campo de aplicação
   Essa Instrução de Trabalho tem como objetivo descrever a política desde a Concepção (Privacy By Design) e Privacidade por Padrão (Privacy by Default);
   Garantindo segurança, definição e controle de acesso desde a primeira coleta dos dados/liberação, evitando assim acessos indevidos e vazamentos de dados.

2. Abrangência
   As regras e diretrizes aqui estabelecidas deverão ser seguidas por todos os colaboradores da Sulplast e seus terceiros que utilizando qualquer tipo de serviço informatizado.

3. Diretrizes do uso de senhas:

a) O usuário é exclusivamente responsável pela utilização de suas credenciais de acesso. A senha, como principal mecanismo de autenticação, deve ser individual, intransferível e mantida em absoluto sigilo. O usuário é responsável por todas as transações realizadas sob sua identificação. Portanto, é fundamental nunca compartilhar a senha com terceiros, incluindo gestores, e jamais permitir que outra pessoa utilize os sistemas da Sulplast autenticados com suas credenciais.

b) É crucial evitar o tráfego de senhas por meio de mensagens de e-mail, chamados ou aplicativos de mensagens instantâneas, bem como evitar anotá-las ou armazená-las em dispositivos móveis, exceto em aplicativos específicos com forte criptografia.

c) Os sistemas, serviços e dispositivos da Sulplast devem ser configurados para atender aos seguintes requisitos mínimos de segurança de senha:

- Devem conter os requisitos mínimos de complexidade:
- No mínimo 8 caracteres
- 1 Letra Maiúscula [A] a [Z];
- 1 Letra minúscula [a] a [z];
- 1 Número [0] a [9];
- 1 Caractere especial [! @ # $ % ^ & * ( ) _ + { } [ ] : ; < > , . ? \ / -];
- Não permitir o uso das 3 últimas senhas cadastradas;
- Obrigatoriamente alterar a senha a cada 180 dias;
- Após 5 tentativas de acesso com senha incorreta, a conta do usuário é bloqueada;

- O bloqueio permanece por 30 minutos, sendo a conta automaticamente desbloqueada após esse período para mais 5 tentativas de acesso.

d) Todas as solicitações de acesso devem ser feitas por meio de chamado aberto diretamente no GLPI e devidamente autorizadas pelo gestor imediato.

e) Os pedidos de recuperação de senhas, por esquecimento ou outros motivos, devem ser feitos através de chamado do GLPI o pelo ramal 114, e seguir um procedimento de validação das informações do usuário para garantir o reset das novas senhas.

f) As senhas iniciais devem ser entregues diretamente aos usuários e configuradas de forma que, no primeiro acesso, seja exigida automaticamente a troca da senha.

g) Acessos a sistemas externos como por exemplo VPN, deverá ter autenticação de dois fatores.

3.1 Senhas de Uso Privilegiado

a) Todas as contas de alto privilégio (por exemplo: administrador, root, etc.) devem ter suas senhas alteradas, renomeadas e desativadas.

b) Para garantir a segurança, apenas um número mínimo de usuários designados como administradores terão acesso privilegiado para essas funcionalidades.

c) Se não for possível alterar ou renomear as senhas das contas privilegiadas, elas serão desativadas e consideradas como "contas de serviço", não utilizadas para qualquer tipo de acesso.

d) Evite introduzir senhas em linhas de comando (códigos-fonte) ou em scripts abertos. Se possível, as senhas devem ser criptografadas e tratadas como "contas de serviço".

e) Todas as senhas em trânsito, ou seja, aquelas transmitidas pela rede, devem obrigatoriamente ser criptografadas.

3.2 Boas práticas na geração de senhas:

Evite utilizar:

Identificações pessoais como nomes, sobrenomes, dados familiares, números de documentos, telefones, placas de carro ou datas especiais.

Sequências previsíveis no teclado (por exemplo: asdfg123).

Palavras comuns encontradas em dicionários, nomes de equipes esportivas, músicas, produtos ou personagens de filmes.

Utilize:

Números aleatórios.

Diversos tipos de caracteres diferentes.

Caracteres especiais.

Substituição de letras por números visualmente similares.

Modificação da primeira, segunda ou última letra de cada palavra. Por exemplo, a frase " Marcha Soldado " pode gerar a senha “M4rch4 Sold4d0.

Políticas de licenciamento e análise de ciclo de vida hardware/software

Avaliação Inicial:

1. Levantamento e Inventário: Realizar um inventário detalhado de todos os ativos de hardware e software na empresa. Verificar se o inventário realizado de forma automático no GLPI está de acordo com todos os hardwares da empresa
2. Análise de Licenças Atuais: Revisar e documentar as licenças existentes para cada software e hardware. Verificar se o cadastro de software e hardware do GLPI está documentado corretamente com o cenário atual.

   Políticas e Procedimentos:

   Política de Aquisição: Verificar a necessidade de novas aquisições. Analisando se o software ou hardware não possui mais atualizações e se a falta deles podem causar algum problema de segurança para a empresa. Levantar no mercado os softwares e hardwares atuais para o serviço que for executado.
   Política de Uso de Software: Cada software deverá possuir suas próprias regras e definições para cada grupo de usuário ou usuários autônomos.
   Política de Atualização e Manutenção: Verificar constantemente se os softwares estão recebendo novas atualizações, e conforme o fabricante qual é sua vida máxima de suporte nas atualizações se estão dentro dos termos das licenças. Também verificar se o hardware está em condições de uso e suportável para receber novas atualizações de software.
   Política de Descarte: Sempre quando for realizar a desativação de um equipamento, garantir que ele não levará consigo nenhum dado pessoal sensível e efetuar o descarte de forma correta. Ao desativar softwares avaliar se existem dados em BD, se eles já foram transferidos para softwares mais novos ou se não irá causar nenhum risco de vazamento de dados

Políticas de Segurança e regulamentos

1. Política de Acesso e Controle:

Autenticação e Autorização: Definição de senhas fortes, autenticação de múltiplos fatores, e acesso baseado em funções. Verificar se o usuário está com acessos ao sistema apenas ao que lhe foi designado.
Gerenciamento de Contas: Procedimentos para criação, modificação e desativação de contas de usuário. Para cada usuário novo/remanejamento ou desligamento utilizamos a IT 1202

2. Política de Proteção de Dados:

Classificação de Dados: Identificação e classificação dos dados sensíveis da empresa.
Manuseio de Dados: Restrições sobre como os dados são coletados, armazenados, usados e compartilhados. Conforme a IT 765 devemos seguir as tratativas de tratamento de dados em conformidade com a LGPD.

3. Política de Segurança de Rede:

Firewalls e Segurança de Rede: Estabelecer diretrizes para a configuração e monitoramento de firewalls, VPNs e outros dispositivos de segurança de rede.
Monitoramento de Tráfego: Regulamentos sobre a análise regular de tráfego de rede para detectar atividades suspeitas.

4. Política de Dispositivos e Ativos:

BYOD (Bring Your Own Device): Diretrizes para dispositivos pessoais conectados à rede da empresa.
Gerenciamento de Ativos: Procedimentos para inventário, manutenção e descarte de ativos de hardware.

5. Política de Educação e Conscientização:

Treinamento em Segurança: Programas regulares de treinamento para funcionários sobre práticas seguras.
Conscientização: Promoção de uma cultura de segurança, incentivando relatórios de incidentes e práticas proativas.

6. Política de Resposta a Incidentes:

Plano de Resposta a Incidentes: Procedimentos para lidar com incidentes de segurança, incluindo escopo, comunicação e recuperação.

7. Política de Conformidade Legal:

Conformidade com Regulamentos: Garantir que a empresa esteja em conformidade com regulamentações relevantes (como GDPR, LGPD, etc.).

8. Revisão e Atualização da Política:

Revisão Periódica: Definir intervalos regulares para revisar e atualizar a política de segurança para refletir mudanças no ambiente de ameaças e tecnologia.